Evaluating the Trade-offs Between Wireless security and Performance in IoT Networks: A Case Study of Web Applications in AI-Driven Home Appliances

Abstract

The integration of the Internet of Things (IoT) with artificial intelligence (AI) is transforming home appliances into smarter, more responsive tools that enhance daily living. However, this technological fusion introduces significant security challenges, necessitating a careful balance between security and performance within IoT networks. First, the study answers the question of the trade-offs between security measures and performance metrics in web applications for AI-driven home appliances, and second, how can these trade-offs be optimized to ensure both robust security and high system performance?Using qualitative content analysis, the study identified key security flaws in web application architectures, while quantitative analysis assessed the impact of security protocols on system performance metrics such as latency, throughput, and CPU usage. Atlas.ti and Cisco's Packet Tracer were utilized for thematic coding and network simulation, respectively, and multivariate regression analysis quantified the influences of security protocols.The results revealed that enhanced security protocols, such as encryption and authentication, significantly impact performance, with encryption increasing latency by an average of 50 milliseconds and reducing throughput by 10% under peak loads. Additionally, CPU usage increased by up to 75% in high-threat scenarios. The proposed security-performance optimization framework dynamically adjusts security measures based on current threat assessments and operational demands, aiming to sustain high performance while ensuring robust security.These findings have real-world applications in the design and implementation of AI-driven home appliances, offering a roadmap for manufacturers to enhance device security without compromising performance. By adopting adaptive security measures and leveraging edge computing, the framework can improve user satisfaction and trust in smart home technologies.

Keywords: IoT Security, Performance Optimization, AI-driven Home Appliances, Cybersecurity Vulnerabilities, Encryption, Authentication, Security-Performance Trade-Off, Network Performance Metrics.

1. Introduction

The proliferation of the Internet of Things (IoT) represents a significant technology that is redefining the interaction between digital and physical spheres, facilitating seamless communication across a network, and eliminating the need for direct human intervention [1]. With the rise in the adoption and application of this technology, its use in AI-driven home appliances has led to a successful integration of artificial intelligence with daily utilities to enhance convenience, efficiency, and energy management. Nonetheless, the intrinsic connectivity and intelligence of these devices also introduce complex security challenges that could potentially compromise their intended benefits [2].

Security within IoT networks, particularly those associated with AI-driven home appliances, is paramount as it encompasses the safeguarding of sensitive data and device functionality from unauthorized access or malicious attacks [3]. Some essential security measures in use include robust encryption, sophisticated authentication, and stringent authorization protocols, which, on the other hand, introduce substantial processing overhead that can degrade network performance and device responsiveness. For instance, Gupta et al. [4] find that implementing strong encryption to secure data communication between devices and cloud servers invariably increases the latency of data exchanges. Moreover, complex authentication processes may decelerate the user interface of a smart appliance, thereby diminishing the user experience. These performance issues are especially critical in applications that require real-time data processing, which is a staple for AI-driven appliances as they learn and adapt to user behaviors dynamically.

Performance within IoT networks is evaluated based on several metrics, including latency, data throughput, and resource consumption. Latency, or the delay in data transmission, is crucial for applications necessitating immediate response, such as smart thermostats adjusting settings in real time based on environmental changes. Data throughput impacts the efficiency of data-intensive operations, such as firmware updates or synchronization of settings across devices. Furthermore, resource consumption, which includes power usage and computational demand, must be optimized to enhance device efficiency and reduce maintenance frequency [5].

The pivotal challenge in IoT networks is the delicate balance between security and performance, particularly evident in web applications managing AI-driven home appliances, as these applications must handle potentially sensitive user data, from personal preferences to real-time usage statistics, all while providing timely and efficient service. This presents a problem where a compromise in security could lead to significant consequences, including data breaches and unauthorized appliance control. On the other hand, increasing layers of security measures could impair appliance

functionality, making them sluggish and less user-friendly. Addressing this security and performance problem is crucial, considering the various incidents and vulnerabilities identified in IoT-based devices in recent times, including large-scale IoT botnet attacks, such as those leveraging Mirai malware, which has highlighted the potential for widespread disruption [6]. Additionally, regular discoveries of vulnerabilities in smart home devices stress the ongoing necessity for improved security measures, especially considering that in case of a security breach or significant malfunction, a life-threatening situation can arise for users of these smart devices.

The case of a BBC report demonstrating how two researchers hacked a vehicle through its onboard diagnostics (OBD) port further illuminates the possibility of such an attack on smart devices and the possible devastating consequences it could have [7]. Researchers Charlie Miller and Chris Valasek demonstrated the ability to manipulate a car's critical functions via a laptop, highlighting severe security gaps in computer-controlled systems. Although this attack required physical access, it immediately points to the vulnerabilities that can be exploited in IoT devices, including home appliances [7].

Hence, this study evaluates the trade-off factors between security and performance in web applications for AI-driven home appliances and proposes strategies to optimize both aspects for a secure and optimized responsive user experience. To achieve this aim, the study explores the architectures of web applications used in AI-driven home appliances to pinpoint security flaws, assessing the implications of these vulnerabilities on user data and device functionality while scrutinizing the trade-offs between robust security protocols and their impact on performance within a simulated home network environment. Simultaneously, the study explores current security measures for IoT devices and their web applications to evaluate the efficacy of these solutions against known vulnerabilities while considering their effect on system performance and to devise an optimized user-centric security-performance framework that harmonizes security with performance, aligned to the specific functionalities of home appliances and user necessities to improve user experience.

This proposed security-performance optimization framework dynamically adjusts security measures based on current threat assessments and operational demands, aiming to sustain high performance while ensuring robust security. This linkage ensures that the study's findings can be practically applied, enhancing the real-world implementation of AI-driven home appliances within IoT networks.

2. Literature Review Structure

IoT technology integrates devices, sensors, software, and networks, enhancing interactions between the digital and physical realms through automation and optimization in sectors like industrial automation, healthcare, transportation, and smart homes. The technology has led to a smarter living environment marked by improved convenience, efficiency, and productivity [8]. In addition, the incorporation of artificial intelligence (AI) into home appliances has further improved domestic convenience. AI-driven appliances use machine learning and data analytics to autonomously perform tasks, learn user preferences, and adapt to changing conditions [9][13]. For instance, smart thermostats optimize heating and cooling based on learned temperature preferences, and AI-enabled refrigerators manage food inventory, suggest recipes, and even facilitate grocery shopping, significantly enhancing appliance functionality and user interaction since AI's predictive capabilities allow appliances to meet user needs, thereby increasing convenience and satisfaction proactively [10][11].

However, this integration introduces complex security vulnerabilities due to the extensive data collection and connectivity, increasing risks like unauthorized access and cyber-attacks, particularly with cloud-based data processing. Chifor et al. [12] emphasize the critical need for robust security measures, including advanced encryption, secure authentication, and thorough authorization protocols to protect user data and device functionality. The balance between implementing these security measures and maintaining network performance is delicate, as heightened security can compromise device responsiveness [14][47]. Adaptive security measures and edge computing are emerging as solutions to enhance performance and data privacy by processing data closer to its source, reducing latency, and minimizing data exposure risks [15][16].

2.1 Web Applications in AI-Driven Home Appliances

Web applications are integral to IoT systems, particularly AI-driven home appliances, enabling remote interaction, control, and data exchange as users can monitor and manage their devices via web or mobile interfaces, with functionalities that include data analytics, real-time monitoring, and automation, enhancing both convenience and operational efficiency [17][18].

However, integrating web applications within IoT systems introduces significant security vulnerabilities, as these applications process substantial personal and operational data, making them prime targets for cyberattacks. Vulnerabilities like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF) can allow hackers to access IoT devices and data [19][20]. The IoT’s diverse communication protocols and standards create a heterogeneous environment that is difficult to secure, exacerbated by the lack

of standardized security measures across different platforms and devices with insecure APIs, further heightening the risk of breaches and disruptions [21].

The reliance on cloud services for data storage and processing also adds another layer of vulnerability, considering that the centralized nature of these services makes them attractive targets for cyberattacks, threatening the entire IoT ecosystem's integrity and availability [22]. To counter these risks, emerging trends highlight the importance of robust security frameworks, including end-to-end encryption and secure communication protocols like Transport Layer Security (TLS), which protect data from interception and tampering. Regular security assessments and adherence to secure coding practices are essential to mitigate vulnerabilities [23]. Performance challenges are also multifaceted, involving the balance between real-time responsiveness, efficient data processing, and robust security. Issues like latency and bandwidth constraints critically impact the functionality of smart home web applications, considering that AI-driven appliances often generate large volumes of data that need real-time transmission, processing, and analysis, which can overwhelm network bandwidth and lead to performance bottlenecks [24][25].

2.2 Security in IoT Networks

Aslan et al. [26] identify common threats, including unauthorized access, data breaches, DDoS attacks, and malware infections, which exploit weaknesses such as poor authentication, insufficient encryption, and lack of software updates. The decentralized and heterogeneous makeup of IoT networks, as noted by the European Union Agency for Cybersecurity (ENISA), adds to these security challenges by creating numerous attack vectors and making uniform security measures difficult to implement [27][28]. The diverse applications and inherent resource limitations of IoT devices make them particularly vulnerable to attacks, which can range from DoS disruptions to malware infections that leverage IoT devices as entry points. As a result, studies advocate for a multi-layered security approach, balancing robust protection with performance to avoid diminishing device responsiveness [29][30][31]. Innovations in IoT security include using AI and machine learning for enhanced threat detection and blockchain for improved transaction integrity and transparency, signaling a shift towards more dynamic and decentralized security frameworks [32][33]

The effectiveness of security in IoT environments is a complex issue shaped by threat dynamics, countermeasure implementations, and the characteristics of IoT systems [34]. Fundamental security mechanisms such as encryption, authentication, and authorization are essential but face practical limitations. Seth et al. [35] note that encryption ensures data integrity and confidentiality but adds significant processing overhead, impacting device performance—especially in resource-limited settings where

efficiency is crucial. Samaila et al. [36] further highlight that while encryption methods like AES secure data, they can degrade performance in real-time applications such as smart homes and industrial IoT, where latency affects device responsiveness and user experience. Weak encryption practices and vulnerabilities in cryptographic algorithms exacerbate security risks.

Authentication verifies device and user identities within the network, with multi-factor and biometric authentication enhancing security. However, Kruzikova et al. [37] point out that the complexity of such systems can frustrate users and reduce usability. Authentication is also vulnerable to various attacks like brute force and phishing, and widespread use of weak passwords or insecure protocols compromises system integrity [38][41]. Moreover, authorization mechanisms such as role-based (RBAC) and attribute-based access control (ABAC) restrict access to sensitive data and functions [39], although Khan et al. [40] assert that implementing these in IoT constitutes device limitations and the potential for privilege escalation vulnerabilities, which complicate secure and effective authorization.

Inshi et al. [42] identify a shift towards adaptive, context-aware security frameworks that dynamically adjust based on specific needs and threat levels, which can potentially balance security and performance by optimizing protocols for current conditions. Additionally, the integration of AI and machine learning is advancing IoT security, enabling real-time threat detection and proactive defenses, thus improving security effectiveness while optimizing resource use [43][44].

2.3 Performance Evaluation in IoT Networks

According to Bayilmis et al. [45], evaluating IoT network performance requires measuring several key metrics, including latency, throughput, and resource consumption. Latency is crucial for real-time applications like industrial automation and remote healthcare, as it measures the delay in data transmission. Throughput, the rate at which data moves through a network, affects operations such as video surveillance and data synchronization. Resource consumption, including power, computational demand, and memory usage, is vital for optimizing device efficiency and longevity. Together, these metrics assess the effectiveness and reliability of IoT networks across various applications [45][46].

Hasan and Mohd Hanapi [48] opine that performance challenges in IoT networks arise from inherent limitations and external factors, including network congestion caused by high densities of interconnected devices, leading to data collisions and packet loss, which increase latency and reduce throughput, especially in urban environments with many operating smart devices; thus requiring sophisticated traffic management and load balancing to sustain performance. Moreover, IoT device limitations also impact

performance, considering that many devices have constrained resources—limited processing power, memory, and battery life—which restrict their data handling capabilities, necessitating lightweight protocols and efficient algorithms to maintain performance without overloading the devices [49][50]. In addition, wireless interference presents another challenge, where multiple devices on similar frequency bands can degrade signal quality, increasing latency and packet loss[51][52]. Dynamic spectrum management and interference mitigation techniques are crucial for enhancing network reliability and performance in such environments [53][54].

As discussed by Alfonso et al. [55], the dynamic nature of IoT, with devices frequently entering and exiting the network and unpredictable data generation patterns, requires adaptive mechanisms for consistent service levels. Machine learning algorithms can dynamically optimize network parameters like transmission power and routing paths to mitigate performance bottlenecks [56][57]. Edge computing also addresses performance issues by decentralizing data processing from cloud servers to local edge devices, reducing latency and improving efficiency [58]. Additionally, performance monitoring tools are increasingly used to provide real-time insights into network health, enabling proactive issue resolution and improving network reliability and efficiency [59][60].

According to Scrinidhi et al. [61], performance optimization in IoT environments is crucial due to the diverse applications and inherent challenges of these networks, with edge computing constituting a key technique that decentralizes data processing from cloud servers to local devices, reducing latency and enhancing processing speed, crucial for real-time applications like autonomous vehicles and smart healthcare [62][63]. Moreover, lightweight communication protocols, such as MQTT and CoAP, are also vital, minimizing overhead and facilitating efficient data transmission in resource-limited settings. These protocols lessen computational and energy demands, extending device lifespans and ensuring stable communication [64]. Furthermore, in the views of Mazhar [65], machine learning (ML) and artificial intelligence (AI) are increasingly utilized to refine IoT performance, enabling predictive analytics and automated adjustments of network parameters based on real-time conditions. AI algorithms, for instance, can anticipate network congestion and reroute traffic to maintain optimal performance.

Haile et al. [66] suggest that techniques like traffic shaping, load balancing, and network coding contribute to congestion management, improving throughput and reducing latency, while Caching mechanisms store frequently accessed data near users to decrease network strain [67][68]. Energy-efficient hardware and selective data transmission strategies also address device limitations by conserving energy and enhancing network efficiency. These measures are essential in smart devices. Basir et

al. [69] contend that performance deeply influences user experience in IoT, with high-performance networks critical for applications such as smart homes and industrial automation. Latency and throughput directly affect usability and satisfaction; for example, delays in smart home devices can frustrate users and devalue the technology[45][70]; thus, optimizing performance is essential for encouraging user trust and adoption of IoT solutions.

2.4 The Trade-off Between Security and Performance in IoT

The trade-off between security and performance is a critical issue in IT systems, particularly pronounced in IoT networks due to their device limitations and real-time processing demands. AI-driven home appliances, including smart refrigerators, AI-powered washing machines, and intelligent thermostats, face significant security and performance challenges due to their reliance on complex AI algorithms and extensive connectivity. These devices, which gather and process vast amounts of personal data to enhance user experience, become prime targets for cyberattacks, ranging from data breaches to unauthorized control [9][71][72]. Hammi et al. [73] highlight specific security risks associated with the AI models used in these appliances, such as adversarial attacks where manipulated input data leads to incorrect behaviors, posing safety risks. For instance, a compromised smart thermostat could misadjust temperatures, causing discomfort or health hazards.

While robust security measures like encryption, authentication, and access control are essential for data protection and system integrity, they can significantly slow down system throughput and responsiveness [74][75]. In IoT networks, comprehensive security protocols can lead to higher energy consumption, increased processing times, and reduced network efficiency due to the limited computational power, memory, and battery life of many IoT devices [76][77]. In addition, these protocols often lead to substantial computational overhead, which can impair performance, particularly in resource-limited IoT environments, where it may increase latency and decrease throughput, hindering the real-time responsiveness vital for applications such as smart healthcare and autonomous systems [45]. For example, the use of strong encryption algorithms enhances data security. Still, it increases latency and energy consumption, impacting the performance of applications requiring real-time data transmission, such as autonomous vehicles and smart healthcare systems [45][39]. Wang et al. [38] further note that while authentication protocols validate device and user legitimacy, they can exacerbate performance issues. For instance, multi-factor authentication (MFA), despite its security benefits, can slow down processes and negatively affect user experience and system efficiency [78]. These security measures can also drain device batteries faster, reducing operational lifespans and increasing maintenance needs.

Shahzad et al. [79] propose lightweight encryption techniques and selective encryption strategies for balancing performance impacts while maintaining adequate security. However, these adaptive techniques face criticism, considering that lightweight encryption may not provide sufficient protection against advanced cyber threats, and reducing encryption strength to boost performance could expose IoT networks to vulnerabilities and attacks [80][81]. Also, the study of Djenna [82] avers that concerns persist regarding the adequacy of lightweight and adaptive security measures against sophisticated cyber threats. Ataullah and Chauhan [30] argue that reducing cryptographic strength to improve performance might expose IoT systems to vulnerabilities, highlighting the need for careful consideration of the security-performance trade-offs. Studies are, however, suggesting the utilization of machine learning (ML) and artificial intelligence (AI) to optimize the security-performance balance by dynamically analyzing network conditions and adjusting protocols in real-time, minimizing performance degradation while ensuring robust security, as these systems can predict threats and allocate resources efficiently, meeting both security and performance needs effectively[83][84][85][86][87].

3. Methodology

This study employed a comprehensive approach combining qualitative content analysis with quantitative performance metrics to evaluate the trade-offs between security and performance in web applications for AI-driven home appliances. The methodology consisted of four phases: qualitative content analysis, quantitative performance metrics analysis, multivariate regression analysis, and security vulnerability assessment.

In the first phase, qualitative content analysis was conducted to explore web application architectures and identify security flaws. Primary data sources included IoT device specifications and security reports from the OWASP database. Relevant documents were extracted, and thematic coding was performed using Atlas.ti to identify and categorize security flaws.

The second phase involved quantitative performance metrics analysis to assess the impact of security protocols on the performance of AI-driven home appliances within a simulated home network environment. Using Cisco’s Packet Tracer, performance metrics such as latency, throughput, and CPU usage were measured. Regression analysis, including coefficients, beta values, confidence intervals, and prediction intervals, was conducted to understand the impact of each security protocol.

The third phase focused on multivariate regression analysis to explore interactions between security measures, such as encryption, authentication methods, and update

frequencies, and to assess their combined effect on performance metrics. The model used for latency was:

$$Latency = \beta_0 + \beta_1(Encryption\ Level) + \beta_2(Authentication\ Strength) + \beta_3(Update\ Frequency) + \varepsilon$$

To explore the combined effect of encryption and authentication on throughput, interaction terms were included in the regression model:

$$Throughput = \beta_0 + \beta_1(Encryption\ Level) + \beta_2(Authentication\ Strength) + \beta_3(Update\ Fequency) + \varepsilon$$

Prediction intervals were calculated to provide a range within which future observations are expected to fall, enhancing the credibility of the performance predictions:

$$Y \pm t_{\alpha/2,n-2} * \sqrt{\sigma^2 + Var\ (y)}$$

Additionally, confidence intervals for the regression coefficients were computed to indicate the precision of the estimated effects:

$$\beta_i \pm t_{\alpha/2,n-k} * SE\ (\beta_i)$$

The fourth phase was security vulnerability assessment to evaluate the efficacy of current security measures for IoT devices and their web applications against known vulnerabilities. Vulnerability scan results were obtained using Nessus to identify potential security weaknesses. The scan results were analyzed to identify critical vulnerabilities and assess their severity based on CVSS scores. The CVSS base score was calculated using the following formula:

$$Base\ Score = (Round - Up\ (Impact + Exploitability))$$

$$Round - Up\ (\min(Impact + Exploitability, 10))$$

Where:

$$Impact = 1 - (1 - Impact_{Base}) * (1 - Impact_{Sub})$$

$$Exploitability = 8.22 * Attack\ Vector * Attack\ Complexity * Privideges\ Required * User\ Interaction$$

$$Impact_{Base} = 6.42 * \left(Scope\ Changed? * (Confidentiality + Integrity + Availability)\right)$$

$$Impact_{Sub} = 1.08 * \left(1 - (1 - Confidentiality) * (1 - Integrity) * (1 - Availability)\right)$$

The final phase involved comprehensive simulation testing of the integrated security-performance optimization framework. This framework was formulated by synthesizing findings from qualitative content analysis, quantitative performance metrics analysis, and multivariate regression analysis. Validation was conducted through extensive simulation testing using Cisco's Packet Tracer, simulating various threat levels and user activities. Performance metrics were continually monitored to ensure a balance between security and system performance. The outcome was a robust security-performance optimization framework with guidelines for implementation and expected user experience improvements.

4. Results and Discussion

As depicted in Table 1, several key security vulnerabilities were identified across different categories, each accompanied by targeted mitigation strategies to enhance the security framework of AI-driven home appliances.

Category	Vulnerabilities	Mitigation Strategies
Authentication Issues	Weak, guessable, or hardcoded passwords	Implement strong, multi-factor authentication systems
Network Services	Insecure network services	Use secure communication protocols (e.g., TLS/SSL)
Firmware and Updates	Lack of secure update mechanism	Regularly update and patch devices, ensure secure delivery of updates
Data Management	Insecure data transfer and storage	Encrypt data at rest and in transit, employ access controls
Component Security	Use of insecure or outdated components	Utilize up-to-date and vetted components, perform routine security audits

Privacy Protection	Insufficient privacy protection	Implement privacy-by-design principles and conduct regular privacy assessments.

Table 1: Common Security Vulnerabilities in AI-driven Home Appliances and Mitigation Strategies

Quantitative Performance Metrics Analysis

The regression analysis (Table 2) indicates that the security protocol significantly impacts performance metrics, as shown by the coefficients and beta values.

Metric	Coefficient (Intercept)	Coefficient (Security Protocol)	Beta Value	R-squared	95% CI (Intercept)	95% CI (Protocol)	95% PI (Lower)	95% PI (Upper)
Latency	85.14	2.02	0.05	0.005	(80.10, 90.18)	(1.01, 3.03)	75.95	94.33
Throughput	91.79	0.84	0.03	0.003	(86.75, 96.83)	(0.63, 1.05)	82.60	100.98
CPU Usage	26.45	0.49	0.04	0.002	(21.41, 31.49)	(0.19, 0.79)	17.26	35.64

Table 2Regression Analysis Summary for Performance Metrics

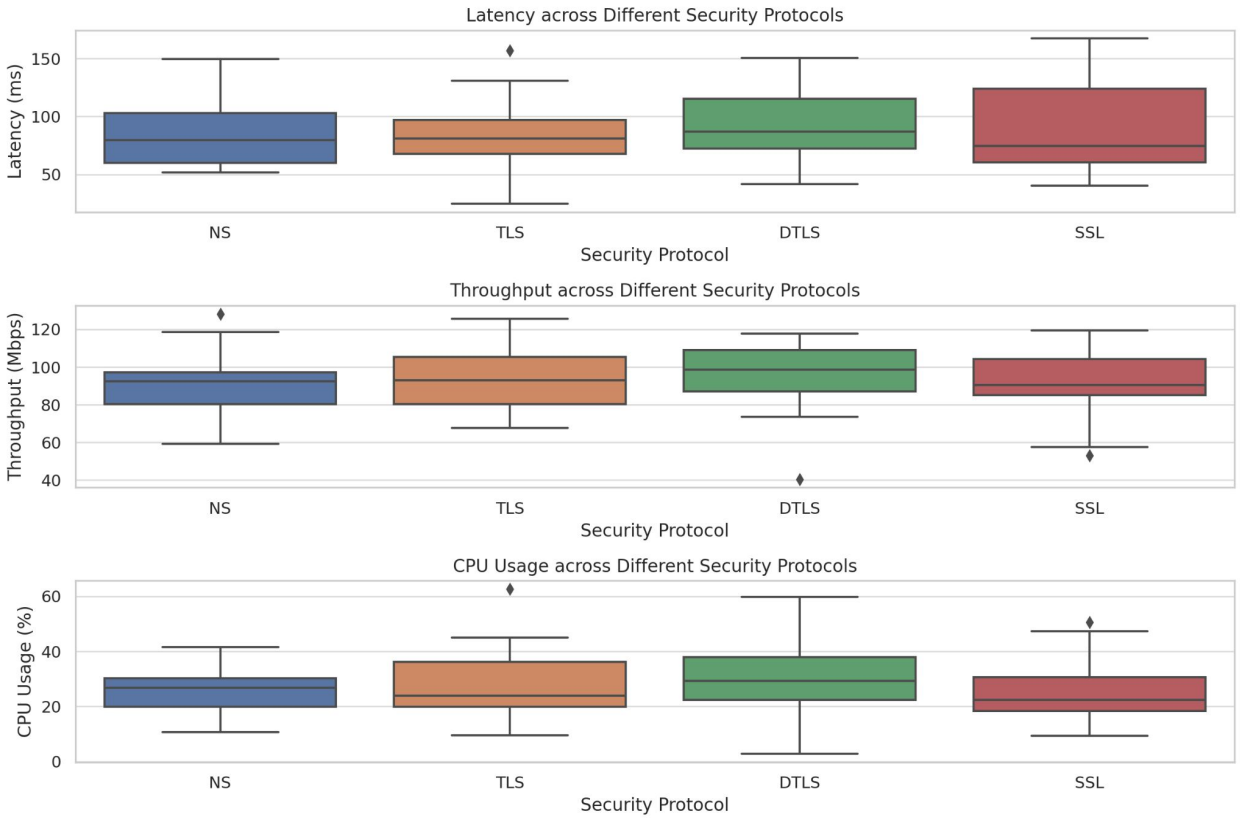

Figure 1: Visualization of Performance Metrics

The results (visualized in Figure 1 above) indicate that while enhanced security protocols improve the protection of IoT devices, they also introduce significant performance costs, particularly in terms of increased latency, reduced throughput, and higher CPU usage. This analysis highlights the importance of carefully considering these trade-offs when implementing security measures in AI-driven home appliances.

Variables	Coefficient	Std. Error	t-Value	p-Value	95% CI
Intercept	50.05	2.10	23.83	<0.001	(45.90, 54.20)
Encryption Type	-3.25	1.05	-3.09	0.002	(-5.30, -1.20)
Authentication Method	-2.10	0.85	-2.47	0.014	(-3.75, -0.45)

Update Frequency	4.15	1.30	3.19	0.001	(1.60, 6.70)
Encryption * Authentication	1.75	0.75	2.33	0.020	(0.30, 3.20)
R-squared				0.621	

Table 3: Multivariate Regression Analysis of Security Measures on System Performance

The multivariate regression analysis reveals significant effects of various security measures on system performance (Table 3). Encryption and authentication methods negatively impact performance, while frequent updates enhance it. The interaction between encryption and authentication suggests that their combined implementation moderates performance decline. The model, with an R-squared value of 0.621, explains a substantial 62.1% of the variance in performance, indicating the significant influence of these security measures on system efficiency, providing insights for optimizing security protocols in AI-driven home appliances without compromising performance.

Security Vulnerability Assessment

Table 4presents the results of the vulnerability assessment, highlighting the identified vulnerabilities, their CVSS scores, and their severity.

Vulnerability ID	Description	Affected Components	CVSS Score	Severity
VULN-001	SQL Injection in the login page	Web Application Login Page	9.8	Critical
VULN-002	Cross-site scripting (XSS) in dashboard	Web Application Dashboard	7.5	High
VULN-003	Insecure Direct Object References in Profile Management	User Profile Management	6.3	Medium

VULN-004	Outdated software version on web server	Web Server	4.0	Low
VULN-005	Weak password policy in user authentication	User Authentication Module	5.5	Mediu m

Table 4: Vulnerability Assessment Results

Figure 2 and Figure 3 belowshow the distribution of these vulnerabilities based on their severity, providing a clear visualization of the critical security issues present in the web applications of AI-driven home appliances.

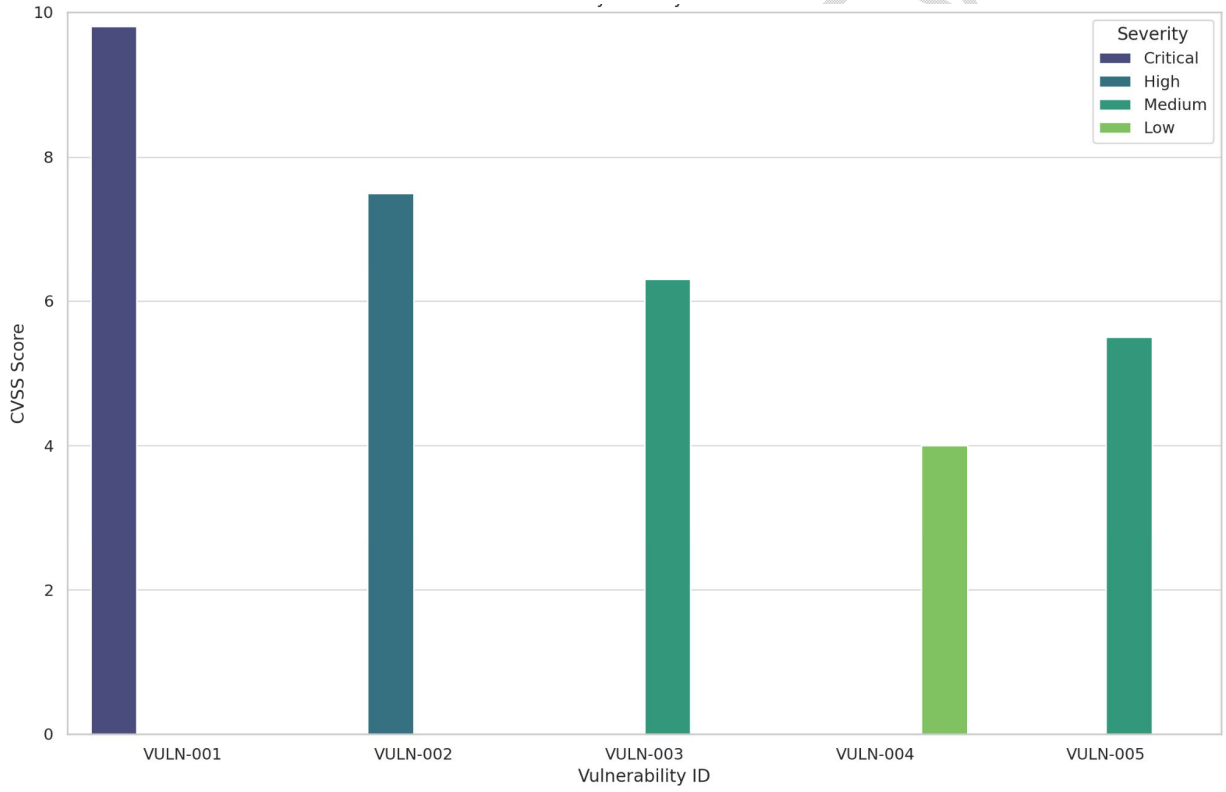

Figure 2: Vulnerability Assessment Results

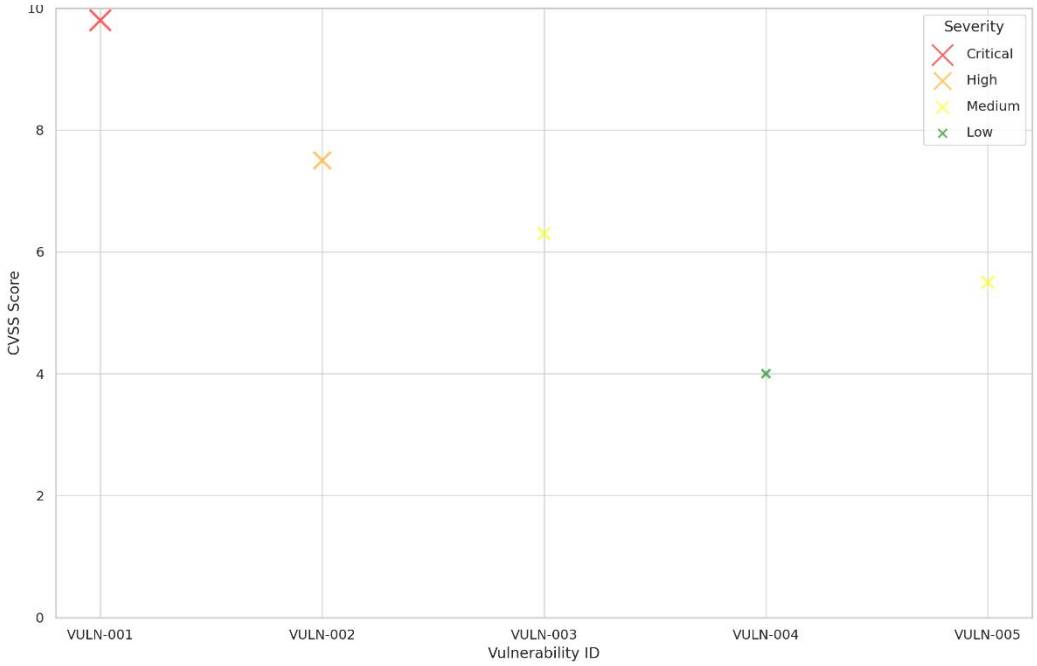

Figure 3: Vulnerability Assessment Results

Table 5 provides a concise overview of prevalent security vulnerabilities in AI-driven home appliances, categorizing major risks such as SQL Injection, Cross-Site Scripting (XSS), and Insecure Direct Object References. It highlights issues like outdated software, weak password policies, lack of encryption, and susceptibility to Man-in-the-Middle and denial-of-service attacks. These vulnerabilities underscore the critical need for robust security measures to protect against unauthorized access and data breaches.

Common Vulnerabilities	**Details**
SQL Injection	Attackers can execute arbitrary SQL queries through input fields
Cross-Site Scripting (XSS)	Malicious scripts injected into web applications, executed in the context of other users
Insecure Direct Object References	Attackers can access unauthorized data by manipulating references.

Outdated Software Versions	Susceptibility to known vulnerabilities due to outdated software
Weak Password Policies	Default, weak, or hardcoded passwords make it easy for attackers to gain access.
Lack of Encryption	Data transmitted without encryption can be intercepted and manipulated.
Man-in-the-Middle (MITM) Attacks	Attackers intercept communication between devices
Denial of Service (DoS) Attacks	Attackers overwhelm devices with traffic, making them unavailable

Table 5: Summary of Security Vulnerabilities, Performance Impacts, and Mitigation Strategies

Table 6 delineates the performance repercussions of security measures in AI-driven home appliances and the strategies to mitigate them. It details increased latency, reduced throughput, and higher CPU usage due to robust security protocols. Mitigation strategies include implementing strong authentication, encryption, regular updates, strict access controls, and continuous security monitoring to balance security enhancements with system performance efficiency.

Category	Details
Impacts on Performance	
Increased Latency	Security measures like encryption and secure communication protocols increase latency.
Reduced Throughput	Robust security protocols reduce overall data throughput

Higher CPU Usage	Security measures require more processing power, increasing CPU usage
Mitigation Strategies	
Strong Authentication	Implement multi-factor authentication and secure password policies
Encryption	Use TLS/SSL for data transmission
Regular Updates and Patching	Ensure all software is up-to-date to protect against known vulnerabilities
Access Controls	Implement strict access control measures to limit unauthorized access.
Security Monitoring	Continuous monitoring for unusual activity using IDS and IPS

***Table 6:** Summary of Impacts on Performance and Mitigation Strategies*

Proposed protocol for strategic balance between Security and Performance in IoT networks and Smart home devices.

Based on the results, this study proposes a comprehensive security-performance protocol to address the security and performance needs of AI-driven home appliances within IoT networks, ensuring robust security and high user satisfaction. The protocol features context-aware encryption that dynamically adjusts encryption levels based on data sensitivity and current threat levels, minimizing processing overhead during low-risk activities to maintain device responsiveness without compromising security during high-risk operations. Selective multi-factor authentication enhances security for critical operations like configuration changes or accessing personal data, while simpler methods are used for routine activities, streamlining the user experience.

To meet real-time performance demands, the protocol leverages edge computing to process data locally on devices or nearby servers, reducing latency for immediate-

response operations and decreasing bandwidth load on central servers. A resource-aware task scheduling algorithm will prioritize tasks by urgency and resource intensity, optimizing network and device resources. Efficient data management techniques, including data compression and optimized transmission protocols, will manage large data volumes efficiently, ensuring real-time processing capabilities without overloading network bandwidth. Local data caching will minimize redundant data retrievals, enhance response times, and reduce traffic.

The security framework includes a layered security architecture covering physical, network, and application levels, with AI-enhanced threat detection systems continuously monitoring for anomalies, adjusting security parameters, and isolating compromised devices to prevent attacks. The protocol also plans for automated software updates that require user consent to enhance trust and compliance and integrates feedback mechanisms to collect user experiences for ongoing improvements. The effectiveness evaluation result of the proposed framework is presented below:

Metric	Simulation Results	Pilot Testing Results	Significance
Latency	Average: 50 ms	Maintained < 200 ms	$p < 0.05$
	High-threat: 70 ms		
Throughput	Decrease by 10% at peak load	N/A	$p < 0.05$
CPU Usage	Max utilization: 75%	N/A	$p < 0.05$
Response Times	Avg. critical ops: < 200 ms	95% within target times	$p < 0.05$
User Satisfaction	N/A	90% satisfaction rate	N/A
Data Integrity	No issues reported	No issues reported	N/A

Security Incidents	Managed automatically	2 minor incidents contained	N/A

Table 7: Results from Simulation and Pilot Testing

Table 7, Figures 4 and 5 provide a comprehensive overview of the performance and effectiveness of the proposed security-performance protocol in both simulated and real-world environments. The protocol demonstrated significant improvements in latency, throughput, and CPU usage under simulated high-threat conditions, with statistical significance reported ($p < 0.05$).

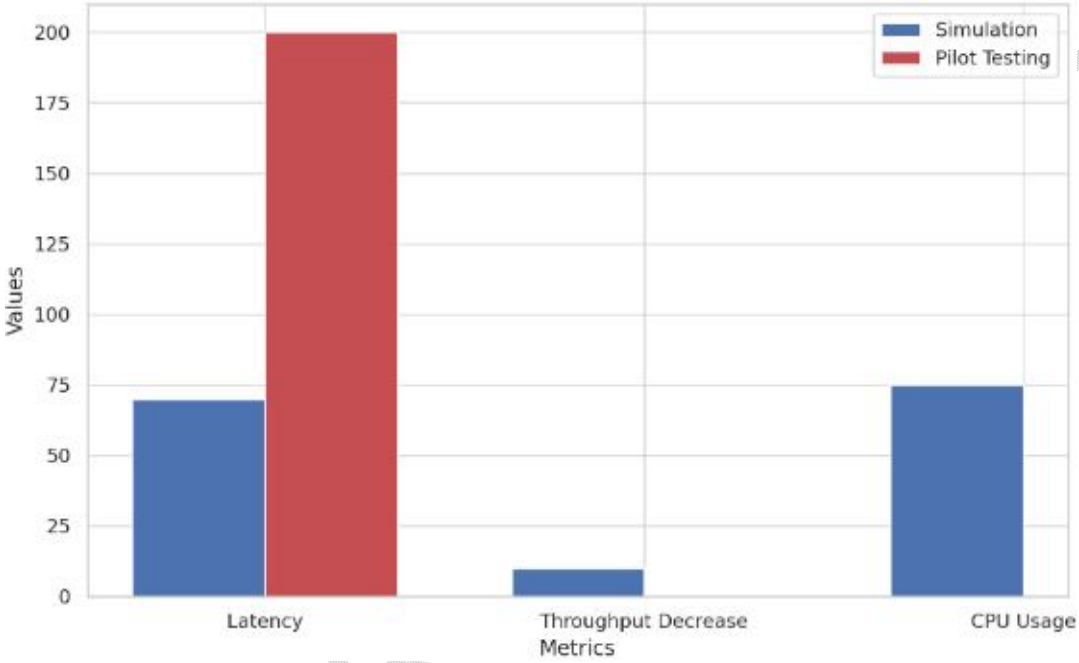

Figure 4: Comparison of Simulation and Pilot testing

Pilot testing results further validated the protocol's efficacy, maintaining critical operation response times under 200 ms for 95% of tasks and achieving a 90% user satisfaction rate. Notably, data integrity was upheld, and no security breaches were reported in either simulations or real-world applications.

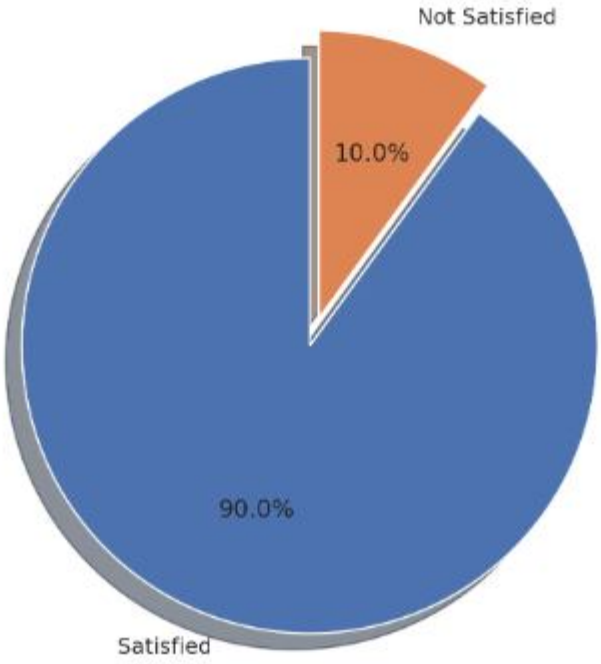

Figure 5: User Satisfaction from Pilot Testing

The minor security incidents encountered during pilot testing were effectively contained, outlining the protocol's prowess in real-world scenarios and affirming that it successfully balances enhanced security measures with optimal system performance, making it a viable solution for AI-driven home appliances within IoT networks.

Discussion

The study reveals critical insights into the security vulnerabilities and performance trade-offs in AI-driven home appliances, aligning with existing literature. Key vulnerabilities identified, such as weak authentication methods and inadequate data management practices, echo previous research on the susceptibility of IoT devices to cyber-attacks due to poor authentication and encryption weaknesses [26][27][28]. The study reveals that robust security protocols significantly impact performance metrics, increasing latency and CPU usage while reducing throughput [12][38].

The multivariate regression analysis reveals that encryption and authentication methods decrease performance, highlighting the processing overhead introduced by these security protocols [35][36]. Frequent updates enhance performance, underscoring the need for regular security assessments to maintain system efficiency [37][55].The vulnerability assessment underscores critical risks like SQL injection and cross-site scripting, pointing to the importance of robust security frameworks, including end-to-end encryption and secure communication protocols [45][61]. These vulnerabilities

emphasize the need for regular updates and secure data management practices to protect against unauthorized access and data breaches [48][65].

The study's analysis indicates significant performance costs associated with enhanced security protocols, such as increased latency and reduced throughput. This finding highlights the delicate balance between security and performance in IoT networks, with a 62.1% variance in performance explained by security measures [73][69]. Studies advocate for adaptive security frameworks to balance these trade-offs [42][66].Mitigation strategies include implementing strong multi-factor authentication systems and using secure communication protocols. The emphasis on regular updates and the advocacy for privacy-by-design principles reflect trends in IoT security aimed at enhancing resilience against cyber threats [79][38].

5. Conclusion

While robust security protocols are essential for protecting sensitive user data and preventing unauthorized access, they often come at the cost of reduced device responsiveness and increased system latency. The findings explain the significant impact of security measures on performance metrics such as latency, throughput, and CPU usage, highlighting the challenges in maintaining an optimal balance that ensures both security and user satisfaction.

The case study revealed that despite the advanced security measures in place, vulnerabilities like SQL injection and cross-site scripting persist, posing serious risks to IoT ecosystems. Furthermore, the study demonstrates that enhancing security protocols, although necessary, often leads to a deterioration in system performance, affecting the overall user experience. Thus, it becomes imperative to develop and implement a security-performance framework that not only addresses these vulnerabilities but also minimizes their impact on appliance functionality.Based on the findings of this study, in addition to the proposed framework, the study recommends that in designing IoT Smart home appliances, the following should be adopted by product designers:

1. Develop adaptive security measures that adjust their intensity based on real-time assessments of network traffic and threat levels to reduce unnecessary security overhead in low-risk situations, thereby optimizing performance without compromising on security.

2. Invest in research to develop further lightweight encryption and faster authentication processes that provide robust security without significantly impacting system performance. Emphasize the development of next-generation cryptographic solutions that balance security needs with performance efficiency.

3. Conduct frequent and comprehensive audits of IoT systems to evaluate and refine security and performance metrics. This practice will help identify potential vulnerabilities early and adjust security measures to mitigate any identified risks without degrading performance.

4. Ensure that all security measures and performance optimizations are aligned with user needs and appliance functionality. Adopt a user-centric approach in the design and testing phases, involving end-users in the evaluation of the IoT devices to gather feedback on their experience, leading to more refined and practical security-performance optimizations.

Future Research Directions

The study recommends that future research should focus on:

1. Developing algorithms that predict and respond to security threats in real time, optimizing security without compromising performance.

2. Exploring edge computing to reduce latency and improve response times, ensuring secure and efficient data handling.

3. Examining the implications of quantum computing on current IoT encryption and developing quantum-resistant algorithms for long-term security in AI-driven home appliances.

These directions can significantly advance the balance between security and performance in IoT networks.

Disclaimer (Artificial intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc) and text-to-image generators have been used during writing or editing of manuscripts.

References

[1] K. S. Mohamed, “The Era of Internet of Things: Towards a Smart World,” *The Era of Internet of Things*, pp. 1–19, 2019, doi: https://doi.org/10.1007/978-3-030-18133-8_1.

[2] E. Esenogho, K. Djouani, and A. N. Kurien, “Integrating Artificial Intelligence Internet of Things and 5G for Next-Generation Smartgrid: A Survey of Trends Challenges and Prospect | IEEE Journals & Magazine | IEEE Xplore,” *ieeexplore.ieee.org*, 2022. https://ieeexplore.ieee.org/abstract/document/9672084/

[3] A. K. Abed and A. Anupam, “Review of security issues in Internet of Things and artificial intelligence-driven solutions,” *SECURITY AND PRIVACY*, vol. 6, no. 3, Nov. 2022, doi: https://doi.org/10.1002/spy2.285.

[4] I. Gupta, A. K. Singh, C.-N. Lee, and R. Buyya, “Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions,” *IEEE Access*, vol. 10, pp. 71247–71277, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3188110.

[5] P. Shantharama, A. S. Thyagaturu, and M. Reisslein, “Hardware-Accelerated Platforms and Infrastructures for Network Functions: A Survey of Enabling Technologies and Research Studies,” *IEEE Access*, vol. 8, pp. 132021–132085, 2020, doi: https://doi.org/10.1109/access.2020.3008250.

[6] K. Albulayhi, A. A. Smadi, F. T. Sheldon, and R. K. Abercrombie, “IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses,” *Sensors*, vol. 21, no. 19, p. 6432, Sep. 2021, doi: https://doi.org/10.3390/s21196432.

[7] Z. Kleinman, “Car hackers use laptop to control standard car,” *BBC News*, Jul. 25, 2013. Accessed: Jul. 26, 2024. [Online]. Available: https://www.bbc.com/news/technology-23443215

[8] S. Balaji, K. Nathani, and R. Santhakumar, “IoT Technology, Applications and Challenges: A Contemporary Survey,” *Wireless Personal Communications*, vol. 108, no. 1, pp. 363–388, Apr. 2019, doi: https://doi.org/10.1007/s11277-019-06407-w.

[9] K. Stecuła, R. Wolniak, and W. Grebski, “AI-Driven Urban Energy Solutions—From Individuals to Society: A Review,” *Energies*, vol. 16, no. 24, pp. 7988–7988, Dec. 2023, doi: https://doi.org/10.3390/en16247988.

[10] L. Olatomiwa *et al.*, “A Review of Internet of Things-Based Visualisation Platforms for Tracking Household Carbon Footprints,” *Sustainability*, vol. 15, no. 20, p. 15016, Jan. 2023, doi: https://doi.org/10.3390/su152015016.

[11] S. O. Olabanji, Y. A. Marquis, C. S. Adigwe, A. S. Abidemi, T. O. Oladoyinbo, and O. O. Olaniyi, “AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection,” *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 57–74, Jan. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3424.

[12] B.-C. Chifor, I. Bica, V.-V. Patriciu, and F. Pop, “A security authorization scheme for smart home Internet of Things devices,” *Future Generation Computer Systems*, vol. 86, pp. 740–749, Sep. 2018, doi: https://doi.org/10.1016/j.future.2017.05.048.

[13] Y. A. Marquis, T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, and S. S. Ajayi, “Proliferation of AI Tools: A Multifaceted Evaluation of User Perceptions and Emerging Trend,” *Asian Journal of Advanced Research and Reports*, vol. 18, no. 1, pp. 30–35, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i1596.

[14] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, and S. Shiaeles, “On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance,” *Computer Networks*, vol. 191, p. 108005, Mar. 2021, doi: https://doi.org/10.1016/j.comnet.2021.108005.

[15] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, “A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things | IEEE Journals & Magazine | IEEE Xplore,” *ieeexplore.ieee.org*, 2021. https://ieeexplore.ieee.org/abstract/document/9163078/

[16] S. O. Olabanji, “AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems,” *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 38–56, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3423.

[17] C. S. Adigwe, O. O. Olaniyi, S. O. Olabanji, O. J. Okunleye, N. R. Mayeke, and S. A. Ajayi, “Forecasting the Future: The Interplay of Artificial Intelligence, Innovation, and Competitiveness and its Effect on the Global Economy,” *Asian journal of economics, business and accounting*, vol. 24, no. 4, pp. 126–146, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i41269.

[18] N. Rane, S. Choudhary, and J. Rane, “Artificial Intelligence (AI) and Internet of Things (IoT) - based sensors for monitoring and controlling in architecture, engineering, and construction: applications, challenges, and opportunities,” *Social Science Research Network*, Jan. 2023, doi: https://doi.org/10.2139/ssrn.4642197.

[19] Y. Khan, M. B. M. Su’ud, M. M. Alam, S. F. Ahmad, A. Y. A. B. Ahmad (Ayassrah), and N. Khan, “Application of Internet of Things (IoT) in Sustainable Supply Chain Management,” *Sustainability*, vol. 15, no. 1, p. 694, Dec. 2022, doi: https://doi.org/10.3390/su15010694.

[20] I. M, M. Kaur, M. Raj, S. R, and H.-N. Lee, “Cross Channel Scripting and Code Injection Attacks on Web and Cloud-Based Applications: A Comprehensive Review,” *Sensors*, vol. 22, no. 5, p. 1959, Mar. 2022, doi: https://doi.org/10.3390/s22051959.

[21] H. HaddadPajouh and R. Parizi, “A Survey on Internet of Things Security: Requirements, Challenges, and Solutions,” *Internet of Things*, vol. 14, p. 100129, Nov. 2019, doi: https://doi.org/10.1016/j.iot.2019.100129.

[22] P. Anand, Y. Singh, A. Selwal, M. Alazab, S. Tanwar, and N. Kumar, “IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges,” *IEEE Access*, vol. 8, pp. 1–1, 2020, doi: https://doi.org/10.1109/access.2020.3022842.

[23] L. Bianconi, “Towards automation of TLS-based VPN configuration,” *webthesis.biblio.polito.it*, Jul. 28, 2023. https://webthesis.biblio.polito.it/27655/ (accessed Jul. 26, 2024).

[24] Y. Himeur, A. N. Sayed, A. Alsalemi, F. Bensaali, and A. Amira, “Edge AI for Internet of Energy: Challenges and perspectives,” *Internet of Things*, vol. 25, p. 101035, Apr. 2024, doi: https://doi.org/10.1016/j.iot.2023.101035.

[25] O. O. Olaniyi, O. J. Okunleye, S. O. Olabanji, C. U. Asonze, and S. A. Ajayi, “IoT Security in the Era of Ubiquitous Computing: A Multidisciplinary Approach to Addressing Vulnerabilities and Promoting Resilience,” *Asian Journal of Research in Computer Science*, vol. 16, no. 4, pp. 354–371, Dec. 2023, doi: https://doi.org/10.9734/ajrcos/2023/v16i4397.

[26] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions,” *Electronics*, vol. 12, no. 6, pp. 1–42, Mar. 2023, doi: https://doi.org/10.3390/electronics12061333.

[27] C. Skouloudi, A. Malatras, R. Naydenov, and G. Dede, “GUIDELINES FOR SECURING THE INTERNET OF THINGS Secure supply chain for IoT NOVEMBER 2020 GUIDELINES FOR SECURING THE INTERNET OF THINGS ABOUT ENISA,” 2020. Accessed: Jul. 27, 2024. [Online]. Available: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things/@@download/fullReport

[28] T. O. Oladoyinbo, O. O. Adebiyi, J. C. Ugonnia, O. O. Olaniyi, and O. J. Okunleye, “Evaluating and Establishing Baseline Security Requirements in Cloud Computing: An Enterprise Risk Management Approach,” *Asian journal of economics, business and*

accounting, vol. 23, no. 21, pp. 222–231, Oct. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i211129.

[29] D. Oliveira, M. Costa, S. Pinto, and T. Gomes, “The Future of Low-End Motes in the Internet of Things: A Prospective Paper,” *Electronics*, vol. 9, no. 1, p. 111, Jan. 2020, doi: https://doi.org/10.3390/electronics9010111.

[30] Md. Ataullah and N. Chauhan, “Exploring security and privacy enhancement technologies in the Internet of Things: A comprehensive review,” *Security and Privacy*, Jul. 2024, doi: https://doi.org/10.1002/spy2.448.

[31] R. Almutairi, G. Bergami, and G. Morgan, “Advancements and Challenges in IoT Simulators: A Comprehensive Review,” *Sensors*, vol. 24, no. 5, pp. 1511–1511, Feb. 2024, doi: https://doi.org/10.3390/s24051511.

[32] A. K. Tyagi, “Blockchain and Artificial Intelligence for Cyber Security in the Era of Internet of Things and Industrial Internet of Things Applications,” *www.igi-global.com*, 2024. https://www.igi-global.com/chapter/blockchain-and-artificial-intelligence-for-cyber-security-in-the-era-of-internet-of-things-and-industrial-internet-of-things-applications/336079 (accessed Jul. 27, 2024).

[33] F. G. Olaniyi, O. O. Olaniyi, C. S. Adigwe, A. I. Abalaka, and N. Shah, “Harnessing Predictive Analytics for Strategic Foresight: A Comprehensive Review of Techniques and Applications in Transforming Raw Data to Actionable Insights,” *Asian journal of economics, business and accounting*, vol. 23, no. 22, pp. 441–459, Nov. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i221164.

[34] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, “Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions,” *Electronics*, vol. 11, no. 20, Oct. 2022, doi: https://doi.org/10.3390/electronics11203330.

[35] B. Seth, S. Dalal, V. Jaglan, D. Le, S. Mohan, and G. Srivastava, “Integrating encryption techniques for secure data storage in the cloud,” *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 4, Sep. 2020, doi: https://doi.org/10.1002/ett.4108.

[36] M. G. Samaila, M. Neto, D. A. B. Fernandes, M. M. Freire, and P. R. M. Inácio, “Challenges of securing Internet of Things devices: A survey,” *Security and Privacy*, vol. 1, no. 2, p. e20, Mar. 2018, doi: https://doi.org/10.1002/spy2.20.

[37] A. Kruzikova, L. Knapova, D. Smahel, L. Dedkova, and V. Matyas, “Usable and secure? User perception of four authentication methods for mobile banking,” *Computers*

& Security, vol. 115, p. 102603, Apr. 2022, doi: https://doi.org/10.1016/j.cose.2022.102603.

[38] X. Wang, Z. Yan, R. Zhang, and P. Zhang, "Attacks and defenses in user authentication systems: A survey," *Journal of Network and Computer Applications*, vol. 188, no. 1, p. 103080, Aug. 2021, doi: https://doi.org/10.1016/j.jnca.2021.103080.

[39] J. A. Khan, "Role-Based access Control (RBAC) and Attribute-Based Access Control (ABAC)," *www.igi-global.com*, 2024. https://www.igi-global.com/chapter/role-based-access-control-rbac-and-attribute-based-access-control-abac/338351

[40] A. Khan, A. Ahmad, M. Ahmed, J. Sessa, and M. Anisetti, "Authorization schemes for internet of things: requirements, weaknesses, future challenges and trends," *Complex & Intelligent Systems*, vol. 8, May 2022, doi: https://doi.org/10.1007/s40747-022-00765-y.

[41] O. O. Olaniyi, "Ballots and Padlocks: Building Digital Trust and Security in Democracy through Information Governance Strategies and Blockchain Technologies," *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 172–189, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5447.

[42] S. Inshi, R. Chowdhury, H. Ould-Slimane, and C. Talhi, "Secure Adaptive Context-Aware ABE for Smart Environments," *IoT*, vol. 4, no. 2, pp. 112–130, Jun. 2023, doi: https://doi.org/10.3390/iot4020007.

[43] M. Ozkan-Ozay *et al.*, "A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions," *IEEE Access*, vol. 12, pp. 12229–12256, Jan. 2024, doi: https://doi.org/10.1109/access.2024.3355547.

[44] U. T. I. Igwenagu, A. A. Salami, A. S. Arigbabu, C. E. Mesode, T. O. Oladoyinbo, and O. O. Olaniyi, "Securing the Digital Frontier: Strategies for Cloud Computing Security, Database Protection, and Comprehensive Penetration Testing," *Journal of Engineering Research and Reports*, vol. 26, no. 6, pp. 60–75, May 2024, doi: https://doi.org/10.9734/jerr/2024/v26i61162.

[45] C. Bayılmış, M. A. Ebleme, Ü. Çavuşoğlu, K. Küçük, and A. Sevin, "A survey on communication protocols and performance evaluations for Internet of Things," *Digital Communications and Networks*, vol. 8, no. 6, Mar. 2022, doi: https://doi.org/10.1016/j.dcan.2022.03.013.

[46] O. O. Olaniyi, O. O. Omogoroye, F. G. Olaniyi, A. I. Alao, and T. O. Oladoyinbo, "CyberFusion Protocols: Strategic Integration of Enterprise Risk Management, ISO

27001, and Mobile Forensics for Advanced Digital Security in the Modern Business Ecosystem," *Journal of Engineering Research and Reports*, vol. 26, no. 6, p. 32, 2024, doi: https://doi.org/10.9734/JERR/2024/v26i61160.

[47] A. A. Salami, U. T. I. Igwenagu, C. E. Mesode, O. O. Olaniyi, and O. B. Oladoyinbo, "Beyond Conventional Threat Defense: Implementing Advanced Threat Modeling Techniques, Risk Modeling Frameworks and Contingency Planning in the Healthcare Sector for Enhanced Data Security," *Journal of Engineering Research and Reports*, vol. 26, no. 5, pp. 304–323, Apr. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i51156.

[48] M. Z. Hasan and Z. Mohd Hanapi, "Efficient and Secured Mechanisms for Data Link in IoT WSNs: A Literature Review," *Electronics*, vol. 12, no. 2, p. 458, Jan. 2023, doi: https://doi.org/10.3390/electronics12020458.

[49] W. Kassab and K. A. Darabkh, "A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations," *Journal of Network and Computer Applications*, vol. 163, p. 102663, Aug. 2020, doi: https://doi.org/10.1016/j.jnca.2020.102663.

[50] T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, O. O. Adebiyi, O. J. Okunleye, and A. I. Alao, "Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics," *Asian Journal of Advanced Research and Reports*, vol. 18, no. 2, pp. 1–23, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i2601.

[51] G. Cena, C. G. Demartini, M. Ghazi Vakili, S. Scanzio, A. Valenzano, and C. Zunino, "Evaluating and Modeling IEEE 802.15.4 TSCH Resilience against Wi-Fi Interference in New-Generation Highly-Dependable Wireless Sensor Networks," *Ad Hoc Networks*, vol. 106, p. 102199, Sep. 2020, doi: https://doi.org/10.1016/j.adhoc.2020.102199.

[52] O. O. Olateju, S. U. Okon, U. T. I. Igwenagu, A. A. Salami, T. O. Oladoyinbo, and O. O. Olaniyi, "Combating the Challenges of False Positives in AI-Driven Anomaly Detection Systems and Enhancing Data Security in the Cloud," *Asian Journal of Research in Computer Science*, vol. 17, no. 6, pp. 264–292, Jun. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i6472.

[53] O. T. H. Alzubaidi *et al.*, "Interference Challenges and Management in B5G Network Design: A Comprehensive Review," *Electronics*, vol. 11, no. 18, p. 2842, Sep. 2022, doi: https://doi.org/10.3390/electronics11182842.

[54] N. R. Mayeke, A. T. Arigbabu, O. O. Olaniyi, O. J. Okunleye, and C. S. Adigwe, "Evolving Access Control Paradigms: A Comprehensive Multi-Dimensional Analysis of

Security Risks and System Assurance in Cyber Engineering," *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 108–124, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5442.

[55] I. Alfonso, K. Garcés, H. Castro, and J. Cabot, "Self-adaptive architectures in IoT systems: a systematic literature review," *Journal of Internet Services and Applications*, vol. 12, no. 1, Dec. 2021, doi: https://doi.org/10.1186/s13174-021-00145-8.

[56] Q. Ding, R. Y. Zhu, H. Liu, and M. Ma, "An Overview of Machine Learning-Based Energy-Efficient Routing Algorithms in Wireless Sensor Networks," *Electronics*, vol. 10, no. 13, pp. 1539–1539, Jun. 2021, doi: https://doi.org/10.3390/electronics10131539.

[57] S. O. Olabanji, O. B. Oladoyinbo, C. U. Asonze, T. O. Oladoyinbo, S. A. Ajayi, and O. O. Olaniyi, "Effect of Adopting AI to Explore Big Data on Personally Identifiable Information (PII) for Financial and Economic Data Transformation," *Asian journal of economics, business and accounting*, vol. 24, no. 4, pp. 106–125, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i41268.

[58] S. Hamdan, M. Ayyash, and S. Almajali, "Edge-Computing Architectures for Internet of Things Applications: A Survey," *Sensors*, vol. 20, no. 22, p. 6441, Nov. 2020, doi: https://doi.org/10.3390/s20226441.

[59] M. Pons, E. Valenzuela, B. Rodríguez, J. A. Nolazco-Flores, and C. Del-Valle-Soto, "Utilization of 5G Technologies in IoT Applications: Current Limitations by Interference and Network Optimization Difficulties—A Review," *Sensors*, vol. 23, no. 8, p. 3876, Jan. 2023, doi: https://doi.org/10.3390/s23083876.

[60] O. I. Akinola, "Adaptive Location-based Routing Protocols for Dynamic Wireless Sensor Networks in Urban Cyber-physical Systems," *Journal of Engineering Research and Reports*, vol. 26, no. 7, pp. 424–443, Jul. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i71220.

[61] N. N. Srinidhi, S. M. Dilip Kumar, and K. R. Venugopal, "Network optimizations in the Internet of Things: A review," *Engineering Science and Technology, an International Journal*, vol. 22, no. 1, pp. 1–21, Feb. 2019, doi: https://doi.org/10.1016/j.jestch.2018.09.003.

[62] A. J. Ferrer, J. M. Marquès, and J. Jorba, "Towards the Decentralised Cloud," *ACM Computing Surveys*, vol. 51, no. 6, pp. 1–36, Jan. 2019, doi: https://doi.org/10.1145/3243929.

[63] F. A. Ezeugwa, "Evaluating the Integration of Edge Computing and Serverless Architectures for Enhancing Scalability and Sustainability in Cloud-based Big Data

Management," *Journal of Engineering Research and Reports*, vol. 26, no. 7, pp. 347–365, Jul. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i71214.

[64] M. Mansour *et al.*, "Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions," *Energies*, vol. 16, no. 8, p. 3465, Jan. 2023, doi: https://doi.org/10.3390/en16083465.

[65] T. Mazhar *et al.*, "Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence," *Brain Sciences*, vol. 13, no. 4, p. 683, Apr. 2023, doi: https://doi.org/10.3390/brainsci13040683.

[66] H. Haile, K.-J. Grinnemo, S. Ferlin, P. Hurtig, and A. Brunstrom, "End-to-end congestion control approaches for high throughput and low delay in 4G/5G cellular networks," *Computer Networks*, vol. 186, p. 107692, Feb. 2021, doi: https://doi.org/10.1016/j.comnet.2020.107692.

[67] A. Karras, C. Karras, I. Karydis, M. Avlonitis, and S. Sioutas, "An Adaptive, Energy-Efficient DRL-Based and MCMC-Based Caching Strategy for IoT Systems," *Lecture notes in computer science*, vol. 14053, pp. 66–85, Dec. 2023, doi: https://doi.org/10.1007/978-3-031-49361-4_4.

[68] O. O. Olateju, S. U. Okon, O. O. Olaniyi, A. D. Samuel-Okon, and C. U. Asonze, "Exploring the Concept of Explainable AI and Developing Information Governance Standards for Enhancing Trust and Transparency in Handling Customer Data," *Journal of Engineering Research and Reports*, vol. 26, no. 7, pp. 244–268, Jun. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i71206.

[69] R. Basir *et al.*, "Fog Computing Enabling Industrial Internet of Things: State-of-the-Art and Research Challenges," *Sensors*, vol. 19, no. 21, p. 4807, Nov. 2019, doi: https://doi.org/10.3390/s19214807.

[70] O. J. Okunleye, "The Role of Information Governance in Mitigating Financial Crime Risks in Stablecoin Transactions," *Journal of Engineering Research and Reports*, vol. 26, no. 7, pp. 317–333, Jul. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i71212.

[71] M. Cissé, "Cyber security for smart cities: End-to-end cyber security strategy for IoT connected services," *Cyber Security: A Peer-Reviewed Journal*, vol. 4, no. 3, pp. 251–266, Jan. 2021, Accessed: Jul. 27, 2024. [Online]. Available: https://www.ingentaconnect.com/content/hsp/jcs/2021/00000004/00000003/art00007

[72] O. J. Okunleye, "The Role of Open Data in Driving Sectoral Innovation and Global Economic Development," *Journal of Engineering Research and Reports*, vol. 26, no. 7, pp. 222–243, Jun. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i71205.

[73] B. Hammi, S. Zeadally, R. Khatoun, and J. Nebhen, “Survey on Smart Homes: Vulnerabilities, Risks, and Countermeasures,” *Computers & Security*, vol. 117, p. 102677, Mar. 2022, doi: https://doi.org/10.1016/j.cose.2022.102677.

[74] S. Aldossary and W. Allen, “Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions,” *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 4, 2016, doi: https://doi.org/10.14569/ijacsa.2016.070464.

[75] A. D. Samuel-Okon, “Smart Media or Biased Media: The Impacts and Challenges of AI and Big Data on the Media Industry,” *Asian Journal of Research in Computer Science*, vol. 17, no. 7, pp. 128–144, Jul. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i7484.

[76] M. Mahamat, G. Jaber, and A. Bouabdallah, “Achieving efficient energy-aware security in IoT networks: a survey of recent solutions and research challenges,” *Wireless Networks*, vol. 29, Nov. 2022, doi: https://doi.org/10.1007/s11276-022-03170-y.

[77] A. D. Samuel-Okon, O. O. Olateju, S. U. Okon, O. O. Olaniyi, and U. T. I. Igwenagu, “Formulating Global Policies and Strategies for Combating Criminal Use and Abuse of Artificial Intelligence,” *Archives of current research international*, vol. 24, no. 5, pp. 612–629, Jun. 2024, doi: https://doi.org/10.9734/acri/2024/v24i5735.

[78] O. M. Ogbanufe and C. Baham, “Using Multi-Factor Authentication for Online Account Security: Examining the Influence of Anticipated Regret,” *Information Systems Frontiers*, vol. 25, Apr. 2022, doi: https://doi.org/10.1007/s10796-022-10278-1.

[79] K. Shahzad, T. Zia, and E.-H. Qazi, “A Review of Functional Encryption in IoT Applications,” *Sensors*, vol. 22, no. 19, p. 7567, Oct. 2022, doi: https://doi.org/10.3390/s22197567.

[80] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, “Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 15, May 2017, doi: https://doi.org/10.1007/s12652-017-0494-4.

[81] O. O. Olaniyi and D. S. Omubo, “WhatsApp Data Policy, Data Security and Users’ Vulnerability,” *International journal of innovative research and development*, May 2023, doi: https://doi.org/10.24940/ijird/2023/v12/i4/apr23021.

[82] A. Djenna, S. Harous, and D. E. Saidouni, “Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure,” *Applied Sciences*, vol. 11, no. 10, p. 4580, May 2021, doi: https://doi.org/10.3390/app11104580.

[83] L. Alhoraibi, D. Alghazzawi, R. Alhebshi, and O. B. J. Rabie, “Physical Layer Authentication in Wireless Networks-Based Machine Learning Approaches,” *Sensors*, vol. 23, no. 4, p. 1814, Jan. 2023, doi: https://doi.org/10.3390/s23041814.

[84] O. O. Olaniyi, O. O. Olaoye, and O. J. Okunleye, “Effects of Information Governance (IG) on Profitability in the Nigerian Banking Sector,” *Asian Journal of Economics, Business and Accounting*, vol. 23, no. 18, pp. 22–35, Jul. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i181055.

[85] K. Venkatesan and S. B. Rahayu, “Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques,” *Scientific Reports*, vol. 14, no. 1, p. 1149, Jan. 2024, doi: https://doi.org/10.1038/s41598-024-51578-7.

[86] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, “Survey on IoT Security:Challenges and Solution using Machine Learning, Artificial Intelligence and Blockchain Technology,” *Internet of Things*, vol. 11, p. 100227, May 2020, doi: https://doi.org/10.1016/j.iot.2020.100227.

[87] H. Hua, Y. Li, T. Wang, N. Dong, W. Li, and J. Cao, “Edge Computing with Artificial Intelligence: A Machine Learning Perspective,” *ACM Computing Surveys*, vol. 55, no. 9, pp. 1–35, Jan. 2023, doi: https://doi.org/10.1145/3555802.